PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-312326
(43)Date of publication of application : 25.10.2002

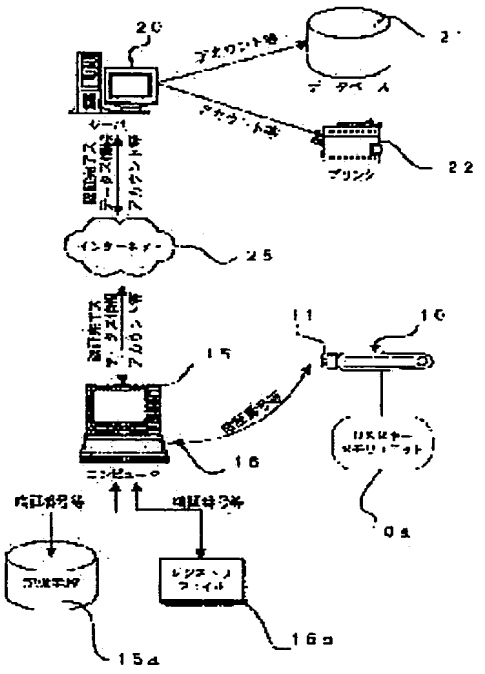
(51)Int.Cl. G06F 15/00
G06F 1/00
G06F 12/14

(21)Application number : 2001-118691
(22)Date of filing : 17.04.2001

(71)Applicant : SMART CARD TECHNOLOGIES:KK
(72)Inventor : TAKEMURA KAZUO

(54) MULTIPLE AUTHENTICATION METHOD USING ELECTRONIC DEVICE WITH USB INTERFACE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a multiple authentication method capable of easily controlling an account and a password, securing high security level, and being applied to various authentication subjects such as a server and a device.
SOLUTION: This multiple authentication method uses an electronic device with an USB interface composed of an account ID authenticating process for reading an account ID from a registry file 15b or a storage means 15a of a target computer 15 and checking the same by the electronic device 10, the computer authentication process, the completion of authentication status information indicating an event that the authentication is completed in both authentication processes, and an access and use rights authentication requiring process for transmitting the account and the password written in a memory unit 10a to the computer 15 as the target of the electronic device or the server 20 or the device 22 connected to the computer 15 by the electronic device 10.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－312326
（P2002－312326A）
(43)公開日　平成14年10月25日(2002.10.25)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ 15/00	３３０Ｃ	５Ｂ０１７
	1/00	３７０	1/00	３７０Ｅ	５Ｂ０８５
	12/14	３２０	12/14	３２０Ｃ	

審査請求　未請求　請求項の数３　ＯＬ　（全８頁）

(21)出願番号　特願2001－118691(P2001－118691)

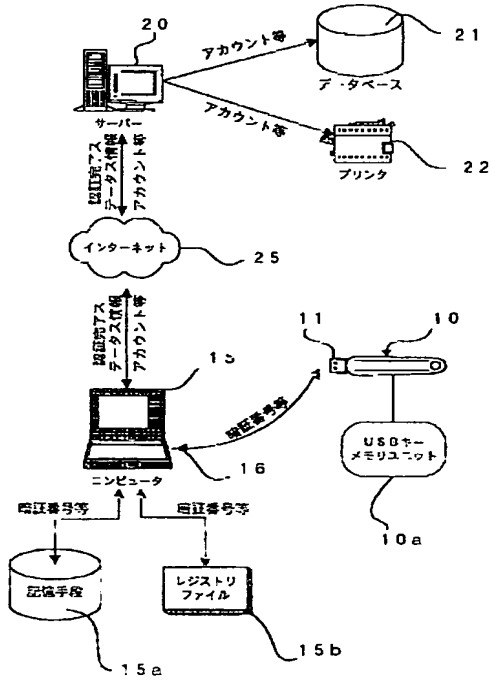
(22)出願日　平成13年４月17日(2001.4.17)

(71)出願人　399001657
株式会社スマートカードテクノロジーズ
千葉県千葉市美浜区中瀬２－６
(72)発明者　竹村　和夫
東京都中央区八丁堀２丁目11番７号　株式会社スマートカードテクノロジーズ内
(74)代理人　100071283
弁理士　一色　健輔　（外３名）

Ｆターム(参考)　5B017 AA03 BA05 BB09
5B085 AE01 AE11 AE23

(54)【発明の名称】　ＵＳＢインターフェイスを備える電子デバイスを用いた複数認証方法

(57)【要約】　（修正有）
【課題】　アカウントやパスワードの管理が簡便であり、高いセキュリティレベルを確保し、サーバー、デバイスなどの多様な認証対象に適用可能な複数認証方法。
【解決手段】　電子デバイス１０が挿入先コンピュータ１５のレジストリファイル１５ｂまたは記憶手段１５ａからアカウントＩＤを読み出して照合するアカウントＩＤ認証過程と、コンピュータ認証仮定と、両方の認証過程で認証が完了した事象を示す認証完了ステータス情報と、コンピュータ１５に接続されるサーバー２０やデバイス２２などに、メモリユニット１０ａに書き込まれたアカウントおよびパスワードとを、電子デバイス１０が当該電子デバイス挿入先のコンピュータ１５しくはサーバー２０やデバイス２２に送信するアクセス・使用権認証要求過程とからなるＵＳＢインターフェイスを備える電子デバイスを用いた複数認証方法。



【特許請求の範囲】
【請求項１】　コンピュータおよびこれに接続される各種サーバーやデバイス、並びに前記コンピュータまたは前記サーバーやデバイスにおいて起動されるアプリケーションプログラムの使用者について、前記コンピュータの備えるＵＳＢポートに接続可能なＵＳＢ端子と、前記使用者を認証するに必要なアカウントやパスワード等の認証情報を記憶したメモリユニットと、前記ＵＳＢ端子を介した前記コンピュータとの前記認証情報の授受・照合処理をコントロールする制御チップセットとを備えたＵＳＢインターフェイスを備える電子デバイスを用いて、その使用可否を判定する認証方法であって、
前記電子デバイスのメモリユニットと、前記コンピュータの記憶手段およびレジストリファイルとに対して書き込み処理された、コンピュータ毎にその使用者と対応付けて設定された暗証番号から生成できるアカウントＩＤのうち、前記コンピュータの記憶手段またはレジストリファイルに書き込まれたアカウントＩＤについて前記電子デバイスが当該電子デバイス挿入先のコンピュータの記憶手段またはレジストリファイルから読み出して、読み出したアカウントＩＤと電子デバイス自身のメモリユニットに格納されている暗証番号から生成できるアカウントＩＤとを照合し、アカウントＩＤ自体の一致不一致を認証するアカウントＩＤ認証過程と、
前記電子デバイスのメモリユニットと、前記コンピュータの記憶手段およびレジストリファイルとに対して書き込み処理された、コンピュータ毎にその使用者と対応付けて設定された暗証番号から生成できるアカウントＩＤのうち、前記記憶手段またはレジストリファイルに書き込まれたアカウントＩＤについて前記電子デバイスが当該電子デバイス挿入先のコンピュータの記憶手段から読み出して、読み出したアカウントＩＤと電子デバイス自身のメモリユニットに格納されている暗証番号から生成できるアカウントＩＤとを照合し、コンピュータと電子デバイスとの個別対応の正当性を認証するコンピュータ認証過程と、
前記アカウントＩＤ認証過程およびコンピュータ認証過程における認証が完了した事象を示す認証完了ステータス情報と、前記コンピュータに接続される各種サーバーやデバイス、並びに前記コンピュータやサーバー等において起動されるアプリケーションプログラムの各々に設定され電子デバイスの前記メモリユニットに書き込まれたアカウントおよびパスワードとを、前記電子デバイスが当該電子デバイス挿入先のコンピュータもしくは前記サーバーやデバイスに送信し、これらサーバーやデバイスならびにアプリケーションプログラムに関するアクセス権および使用権について認証要求するアクセス・使用権認証要求過程とを有することを特徴とするＵＳＢインターフェイスを備える電子デバイスを用いた複数認証方法。

【請求項２】　前記電子デバイスのメモリユニットに書き込まれている、当該電子デバイスに対応するコンピュータがサーバーへ最後に正当なアクセスをした最終接続情報を、前記アクセス・使用権認証要求過程において前記コンピュータもしくは前記サーバーやデバイスに送信することを特徴とする請求項１に記載のＵＳＢインターフェイスを備える電子デバイスを用いた複数認証方法。
【請求項３】　前記暗証番号に加えて他の付帯番号を前記電子デバイスおよびコンピュータに格納し、この暗証番号および付帯番号からアカウントＩＤもしくはアカウントＩＤと付帯ＩＤを生成して、前記アカウントＩＤ認証過程およびコンピュータ認証過程におけるアカウントＩＤの照合を行うことを特徴とする請求項１または２に記載のＵＳＢインターフェイスを備える電子デバイスを用いた複数認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明はＷＥＢサーバーやＡＳＰサーバーなどのサーバコンピュータ、プリンタなどの各種デバイス、およびそれらにおいて起動するアプリケーションプログラムにコンピュータを通じてアクセスする可否を認証する認証方法に関し、特にＵＳＢキーなどのＵＳＢインターフェイスを備える電子デバイスを用いた複数認証方法に関する。
【０００２】
【従来の技術】堰を切ったようにあらゆる業種・業界においてＥコマースサイトが立ち上がり、最近ではコンピュータとそれを結ぶネットワークが企業といわず個人といわず巷にあふれている印象が強い。このように、一般の個人が容易にコンピュータに触れ、誰もが利用しやすいネットワーク環境が整いつつある現況において、ネットワークを含めたコンピュータシステムのセキュリティ管理が重要視されてきている。そこで、着目されるのがコンピュータやネットワークへの不正アクセスやそれにともなうデータの盗用・改変・破壊を防止する認証技術である。
【０００３】従来の認証技術においては、マルチユーザーのコンピュータ・システムやネットワーク・システムを使用する際に正当な使用者たる本人であることを確認するためにユーザーＩＤとパスワードの組み合わせ入力によって認証が実行されていた。使用者がコンピュータ・システムやネットワークにログ・インする際に、ユーザーＩＤとパスワードのデータを入力すると、それがあらかじめアクセス権限リストに登録されたものかどうかの確認（認証）がなされ、認証された場合にのみシステムの使用が許可されることになる。このとき、アクセス権限リストに登録されたレベルのアクセス権限をユーザーに与える。
【０００４】
【発明が解決しようとする課題】ところが、上記のよう

な従来手法による認証では新たに別の問題が浮かんできた。例えば、悪意の第三者によるパスワード等の盗用や解析を防ぎたいと考えるあまりにアカウントやパスワードを頻繁に変更したり大幅な桁数増加を図るとすれば、その管理が使用者本人にも難しくなる問題がある。認証のたびにそれらの桁数の多いパスワード等を手動で入力するのは非常に面倒であるし、頻繁に変更するパスワード等を、多岐にわたる認証対象毎に確実に記憶しておくのは至難の業である。ましてやその認証ステップや桁数が多いとなれば使用者本人の記憶の中だけで管理するのはまず不可能であろう。

【０００５】この場合、メモ帳などに認証対象の種類や変更のたびごとに暗証番号などを記入して当初はそれを逐次参照するしかないが、紙など視認性のある媒体に記録した瞬間に盗用のおそれが生じる。このためこのような手法が適用される状況としては、機密性のそれほど高くないデータしか取り扱わない企業向けや、一人暮らしの個人が密室において遊びでコンピュータを使用するといった、低度のセキュリティレベルしか要しない場面に限定されることになる。

【０００６】また、コンピュータに付帯するキーボード等の入出力インターフェイスを用いて上記パスワードなどの入力作業を行うわけであるが、例えばそこでタイピングした文字・記号のキャラクターデータを経時記録しておき、第三者が後に当時のタイピング状況を再生可能とするプログラムや、目的のサーバーになりすまして偽のWeb画面データをターゲットのコンピュータに送信し、そこで入力されたアカウントやパスワードを抽出して盗用するといった手の込んだケースも存在する。

【０００７】一方、使用者が自らのコンピュータにおいて一度入力したアカウントとパスワードはブラウザやＯＳなどのパスワード記憶機能などによってコンピュータ内に保存可能である。この機能が使用するレジストリファイルなどを第三者が発見するのは容易であるし、もしコンピュータごと盗難された場合にはパスワードなど一切知らずとも各種サーバーやアプリケーションプログラム等に対しアクセス・使用可能となってしまうおそれもある。いずれにせよ、アカウントやパスワードの手入力を省略してもしなくても、セキュリティ面から言えば抜け穴は多く用意されていたのである。

【０００８】本発明はこのような事情に鑑みてなされたものであって、アカウントやパスワードの管理が簡便でありながらも高いセキュリティレベルを確実に確保し、サーバー、デバイス、およびアプリケーションプログラムといった多様な認証対象に幅広く適用可能であるＵＳＢキーを用いた複数認証方法を提供することを目的とする。

【０００９】

【課題を解決するための手段】この発明は上記目的を達成するためになされたもので、第１の発明は、コンピュータおよびこれに接続される各種サーバーやデバイス、並びに前記コンピュータまたは前記サーバーやデバイスにおいて起動されるアプリケーションプログラムの使用者について、前記コンピュータの備えるＵＳＢポートに接続可能なＵＳＢ端子と、前記使用者を認証するに必要なアカウントやパスワード等の認証情報を記憶したメモリユニットと、前記ＵＳＢ端子を介した前記コンピュータとの前記認証情報の授受・照合処理をコントロールする制御チップセットとを備えたＵＳＢインターフェイスを備える電子デバイスを用いて、その使用可否を判定する認証方法であって、前記電子デバイスのメモリユニットと、前記コンピュータの記憶手段およびレジストリファイルとに対して書き込み処理された、コンピュータ毎にその使用者と対応付けて設定された暗証番号から生成できるアカウントＩＤのうち、前記コンピュータの記憶手段またはレジストリファイルに書き込まれたアカウントＩＤについて前記電子デバイスが当該電子デバイス挿入先のコンピュータの記憶手段またはレジストリファイルから読み出して、読み出したアカウントＩＤと電子デバイス自身のメモリユニットに格納されている暗証番号から生成できるアカウントＩＤとを照合し、アカウントＩＤ自体の一致不一致を認証するアカウントＩＤ認証過程と、前記電子デバイスのメモリユニットと、前記コンピュータの記憶手段およびレジストリファイルとに対して書き込み処理された、コンピュータ毎にその使用者と対応付けて設定された暗証番号から生成できるアカウントＩＤのうち、前記記憶手段またはレジストリファイルに書き込まれたアカウントＩＤについて前記電子デバイスが当該電子デバイス挿入先のコンピュータの記憶手段から読み出して、読み出したアカウントＩＤと電子デバイス自身のメモリユニットに格納されている暗証番号から生成できるアカウントＩＤとを照合し、コンピュータと電子デバイスとの個別対応の正当性を認証するコンピュータ認証過程と、前記アカウントＩＤ認証過程およびコンピュータ認証過程における認証が完了した事象を示す認証完了ステータス情報と、前記コンピュータに接続される各種サーバーやデバイス、並びに前記コンピュータやサーバー等において起動されるアプリケーションプログラムの各々に設定され電子デバイスの前記メモリユニットに書き込まれたアカウントおよびパスワードとを、前記電子デバイスが当該電子デバイス挿入先のコンピュータもしくは前記サーバーやデバイスに送信し、これらサーバーやデバイスならびにアプリケーションプログラムに関するアクセス権および使用権について認証要求するアクセス・使用権認証要求過程とを有することを特徴とするＵＳＢインターフェイスを備える電子デバイスを用いた複数認証方法。

【００１０】第２の発明は第１の発明において、前記電子デバイスのメモリユニットに書き込まれている、当該電子デバイスに対応するコンピュータがサーバーへ最後

に正当なアクセスをした最終接続情報を、前記アクセス・使用権認証要求過程において前記コンピュータもしくは前記サーバーやデバイスに送信することを特徴とするＵＳＢインターフェイスを備える電子デバイスを用いた複数認証方法。

【００１１】第３の発明は、第１または第２の発明において、前記暗証番号に加えて他の付帯番号を前記電子デバイスおよびコンピュータに格納し、この暗証番号および付帯番号からアカウントＩＤもしくはアカウントＩＤと付帯ＩＤを生成して、前記アカウントＩＤ認証過程およびコンピュータ認証過程におけるアカウントＩＤの照合を行うことを特徴とするＵＳＢインターフェイスを備える電子デバイスを用いた複数認証方法。

【００１２】

【発明の実施の形態】＝＝＝電子デバイスとしてのＵＳＢキーの構造＝＝＝

ＵＳＢ（Universal Serial Bus)は、パーソナルコンピュータ向けのシリアル・インターフェース規格であって、係る規格に準拠した機器（ＵＳＢ機器）とコンピュータとの接続をコンピュータ側が自動的に認識するプラグ・アンド・プレイ機能や、パーソナルコンピュータや機器の電源を入れたままＵＳＢコネクタの抜き差しが可能となるホット・プラグ機能を可能にしている。また、ある程度までの電源の確保も接続先のコンピュータ等から行うことが出来るため機器自体の小型化を図ることができ、前述の接続処理のし易さとあいまって、扱いやすさの点で非常に優れている。本発明において使用される電子デバイスとしてのＵＳＢキーは前述の機能を備えた上で、複数段階にわたる認証処理を実行可能なよう設計されている。

【００１３】図１はＵＳＢキー１０の外形と使用形態の一例を示す説明図である。本発明の複数認証方法に用いられるＵＳＢキー１０は、外形的には図に示すようなパーソナルコンピュータなど各種コンピュータ１５の備えるＵＳＢポート１６に接続可能なＵＳＢ端子１１と、このＵＳＢ端子１１の端部を固定するとともに人が把持しやすく携帯に便利な例えばスティック状などの種々の形状およびサイズで内部の電子ユニットを衝撃等から保護可能な強度を備えるケーシング１２とからなっている。

【００１４】一方そのケーシング１２内部には、コンピュータ１５の使用者を認証するに必要なアカウントやパスワード等の認証情報を記憶したメモリユニットと、ＵＳＢ端子１１を介したコンピュータ１５との前記認証情報の授受・照合処理をコントロールする制御チップセットとを備えている。両者を一体としたＩＣチップセットなどを想定することもできる。また、前記ケーシング１２とメモリユニットとを構造的に連結し、ケーシング１２をこじ開けるとメモリユニット（もしくはメモリ内容）が破損されるようにすれば、セキュリティ性がより向上するであろう。当然、メモリユニット内に書き込まれている前記認証情報は暗号化されていることが好ましい。

【００１５】＝＝＝本発明を実現するシステム構成＝＝＝

図２は本発明の複数認証方法を実現するシステム構成例を示す説明図である。以下、上記ＵＳＢキー１０を用いた複数認証方法を実際に運用するシステム構成について説明する。ここでは、予め契約した会員だけにアクセスを許すサーバー２０が、インターネット２５を介して前記会員のコンピュータ１５へ各種のアプリケーションプログラムの提供を行うASP（Application Service Provider）として機能する状況を想定する。ASPとして前記サーバー２０が役割を担う際には、当然のことながら会員認証を行って、アクセスする者の正当性を検証しなければならない。一方でその会員らは、サーバー２０へのアクセスの度に要求される認証処理に逐次対応する必要がある。そこで本発明のＵＳＢインターフェイスを備える電子デバイス（例：ＵＳＢキー）を用いた複数認証方法をこの状況に適用し、前記サーバー２０やそこで提供されるアプリケーションプログラムに設定されたアカウントやパスワードの管理を簡便化し、かつ高いセキュリティレベルを確保することとする。

【００１６】サーバー２０は、前述したようにインターネット２５などの情報通信ネットワークに接続し、ASPサーバー、Webサーバーおよび電子メールサーバーとして機能する。また、当サーバー２０の運営者側と契約を交わし会員となった者の個別データをカタログ化して管理する。この個別データには、各会員毎にアカウントが付されて管理され、このアカウントをベースにした、氏名（名称）、契約内容、取引履歴、パスワード等との関係表が作成されている。なおこの関係表における各種情報は前記ＵＳＢキー１０の適宜なメモリに格納される場合もある。

【００１７】他に、会員に提供するアプリケーションプログラムが格納されたデータベース２１を有し、その管理を行っている。ここに格納されるアプリケーションプログラムとしては、複雑なノウハウを蔵した金融工学的計算や科学技術計算、企業における給与計算や税務処理などを実行するプログラムが考えられるが、ASPの業態等に応じて様々である。このようなアプリケーションプログラムは、会員のコンピュータ１５からインターネット２５を通じてサーバー２０に送られてくるリクエストに応えて実行されるものであり、会員は実行に必要なデータのみをサーバー２０に送信することで、例えばサーバー２０が実行した複雑で膨大な計算によって得られた処理結果のみを受け取ることができる。勿論、アプリケーションプログラムを使用させるといったASPとしての機能だけでなく、プリンタ２２やカメラなど各種デバイスを使用させる機能を設定してもよい。

【００１８】上記サーバー２０にインターネット２５な

どを介してアクセスするのがコンピュータ１５である。このコンピュータ１５は使用者（会員）毎に暗証番号などを決めて使用権が設定されるため、コンピュータ起動時などにこの使用権の有無を確認する認証作業を行う必要がある。１台のコンピュータ１５に１人のみ使用権を設定するか複数人の使用権を設定するかは、暗証番号などの認証情報をいくつ発行するかで容易にコントロールできる。また、ハードディスクドライブなどの適宜な記憶手段１５ａを備え、ここにＯＳやブラウザ、メールソフトなど各種アプリケーションをインストールしている。一般にこの記憶手段１５ａ内に、各種の環境設定やドライバの指定、アプリケーションの関連づけなどの情報を保存するレジストリファイル１５ｂが格納されている。本発明において、これら記憶手段１５ａとレジストリファイル１５ｂとには使用者毎に設定された暗証番号が記録されている。

【００１９】上記コンピュータ１５のＵＳＢポート１６に接続されるのが前記ＵＳＢキー１０であり、ＵＳＢ端子１１を介してメモリユニット１０ａに書き込まれている暗証番号から生成できるアカウントＩＤをコンピュータ１５と授受し照合する。

【００２０】なお、コンピュータ１５は一般的なパーソナルコンピュータなどに限定されるものではなく、インターネット接続機能を備えた携帯電話機やＴＶ受像器、ファックス機など様々なコンピュータ機器を、ＵＳＢ接続可能であることを条件に適用することが出来る。

【００２１】＝＝＝実施手順＝＝＝

図３は本発明の複数認証方法の実際手順を示す流れ図である。上で述べたようにサーバー２０がASPサーバーとして機能するものとして以下に本発明の複数認証方法の実施手順を説明する。まずサーバー２０を運営するASP業者と契約し登録された各会員について認証情報を設定する必要がある（ステップｓ２００）。必要な認証情報としては、アカウント、パスワード、および暗証番号である。アカウントとパスワードについては、サーバー２０に会員のコンピュータ１５がログインする際のサーバーログイン用のものと、このサーバー２０を通じて使用するアプリケーションプログラムやそれを格納したデータベース２１およびプリンタ２２などのデバイス等の各使用権を確認する使用権確認用のものとがある。他方、暗証番号は前記会員毎に設定されるものであって、当該使用者が使用するコンピュータ１５とＵＳＢキー１０との使用権についての対応確認に用いられる。

【００２２】前記暗証番号は読みとられても容易に流用されないよう暗号化処理が施され、コンピュータ１５の記憶手段１５ａおよびレジストリファイル１５ｂに対して書き込み処理される（ステップｓ２０１）。次に、前記暗証番号と、ステップｓ２００で設定されたサーバーログイン用および使用権確認用のアカウント・パスワードとを、ＵＳＢキー１０のメモリユニット１０ａに登録する（ステップｓ２０２）。前記暗証番号から生成されるアカウントＩＤによりＵＳＢキー１０の所持者である会員と当該会員が使用するコンピュータ１５との正当な使用関係が後に認証されることになる。

【００２３】そして、ＵＳＢキー１０に対応するコンピュータ１５がサーバー２０へ一度でも正当なアクセスをしたことがあれば、その最終接続情報（例えば最終のクッキー情報）を、前記コンピュータ１５の例えば記憶手段１５ａ内から取得し、該当するＵＳＢキー１０のメモリユニット１０ａに書き込み処理をする（ステップｓ２０３）。サーバー２０へのアクセス初回である場合には、ＵＳＢキー１０が予め備える固有情報でもってこの最終接続情報の書き込み処理は免除されるとすれば好適である。ここまでのステップにてアカウント、パスワード、暗証番号、クッキーといった認証に必要な情報の設定と、各機器への書き込みが完了する。

【００２４】以後、コンピュータ１５を起動した（ステップｓ２０４）前記会員がサーバー２０にアクセスすることを試みる。この会員は、起動されたコンピュータ１５のＵＳＢポート１６に、自ら所持するＵＳＢキー１０を挿入する（ステップｓ２０５）。コンピュータ１５のＯＳはプラグ・アンド・プレイ機能によりＵＳＢポート１６に挿入されたＵＳＢキー１０の認識を始める。そしてコンピュータ１５のシステムへの認識・組み込みが完了したＵＳＢキー１０は、コンピュータ１５の記憶手段１５ａまたはレジストリファイル１５ｂへアクセスする。そしてそこに記録されている前記暗証番号からアカウントＩＤを抽出し、自身のメモリユニット１０ａに格納されている暗証番号から生成できるアカウントＩＤと照合する（ステップｓ２０６：アカウントＩＤ認証過程）。

【００２５】この暗証番号の照合により暗証番号から生成されたアカウントＩＤ自体の一致不一致をみる。また、記憶手段１０ａからも暗証番号から生成できるアカウントＩＤを抽出・照合する（ステップｓ２０７：コンピュータ認証過程）。これらのステップｓ２０６、ｓ２０７におけるアカウントＩＤの照合によりＵＳＢキー１０とコンピュータ１５との対応関係の正当性とアカウントＩＤの正当性とを認証する。いずれかのステップにてアカウントＩＤの不一致をみた場合、ＵＳＢキー１０の制御チップセットは、コンピュータ１５に対してそのＯＳに組み込まれた電源制御機能や各種入力機能の制限を命令し、正当とは認められない者のコンピュータ１５の使用を差し止める。

【００２６】アカウントＩＤ認証過程およびコンピュータ認証過程における認証が正常に完了した場合（ステップｓ２０８）、その完了事象を示す認証完了ステータス情報がＵＳＢキー１０またはコンピュータ１５により発行される（ステップｓ２０９）。この認証完了ステータス情報は、例えばある会員に設定された暗証番号から生

成されるアカウントＩＤについて、対応するコンピュータのレジストリファイルおよび記憶手段において一致が認められた旨のテキストデータが圧縮・暗号化されているものである。この情報の発行は、ＵＳＢキー１０とコンピュータ１５との関係が、使用者たる会員の正当性の面でも、暗証番号由来のアカウントＩＤの正当性の面でも認証されたことを意味する。つまり、権利的に何ら問題ない使用者が、予め定められたコンピュータ１５を正当に使用している状況を指し示す。

【００２７】認証完了ステータス情報を発行したＵＳＢキー１０は、この認証完了ステータス情報、自身のメモリユニット１０ａに書き込まれた前記アカウントおよびパスワード、および前記クッキー情報を、当該ＵＳＢキー挿入先のコンピュータ１５とインターネット２５でつながったサーバー２０やデバイスに送信する（ステップｓ２１０）。これによりこれらサーバーやデバイスは、送られてきたアカウント等の情報を受けて自身が保持しているアカウント等との照合作業を開始することになる。これをアクセス権および使用権についての認証要求とする（ステップｓ２１１：アクセス・使用権認証要求過程）。

【００２８】サーバー２０側では認証完了ステータス情報を読みとってどの会員がどのコンピュータから正当にアクセスを試みているのか認識する。と同時に、サーバーログイン用のアカウント・パスワード、ならびにクッキー情報の一致を認証すればアクセスを許可する。本実施例では、ASPサーバーとしてサーバー２０が機能するから、サーバー２０の記憶手段２１に格納されている各種アプリケーションプログラムの使用権についてのアカウント・パスワード認証も実施する。サーバー２０側での認証が全て正常に完了すればアクセス・使用権認証通知がコンピュータ１５に送信される。コンピュータ１５およびＵＳＢキー１０では前記のアクセス・使用権認証通知を受信し（ステップｓ２１２）、認証完了となる（ステップｓ２１３）。

【００２９】なお、前記アカウントＩＤ認証過程およびコンピュータ認証過程において一致不一致の照合対象となったアカウントＩＤは、両過程において全く同じものを用いても良いし、或いは各過程で由来が別のアカウントＩＤを用いるとしてもよい。

【００３０】また、前記暗証番号に加えて他の付帯番号を前記電子デバイスおよびコンピュータに格納し、この暗証番号および付帯番号からアカウントＩＤもしくはアカウントＩＤと付帯ＩＤを生成して、前記アカウントＩＤ認証過程およびコンピュータ認証過程におけるアカウントＩＤの照合を行うこととしても好適である。

【００３１】＝＝＝その他の実施例＝＝＝

多様な認証手段を統合した複数認証としては、上記実施例のようなアカウントとパスワードおよび暗証番号から生成されるアカウントＩＤによるものに加え、ログイン時に自動的にパスワードを生成するトークン、デジタル証明書、生体認証（指紋や虹彩走査）など多種多様な認証手段の組み合わせを適用することも考えられる。いずれにしてもこれらの認証情報をＵＳＢキーのメモリユニットに格納しておけばよいのである。

【００３２】

【発明の効果】以上に説明したように本発明のＵＳＢインターフェイスを備える電子デバイスを用いた複数認証方法によれば、アカウントやパスワードを頻繁に変更したり、大きな桁数のそれらアカウントやパスワードを認証のたびごとに手入力することなく悪意の第三者によるパスワード等の盗用や解析を防ぐことが可能になる。しかも、たとえそれらアカウントやパスワードを頻繁に変更し、その上その桁数をどれだけ大きく複雑なものとしたとしても、アカウントやパスワード等は電子デバイスのメモリユニットに格納されるため、使用者本人はなんらその複雑さを意識することなく簡便に使用・管理することが出来るのである。

【００３３】また、電子デバイスのメモリ内にパスワード等を記憶するために、メモ帳やノート、手帳といった視認性のある媒体に記録するのとは異なり、容易には盗み見られる状況は生じないし、かといってパソコン内のファイルにパスワード等を暗号化記録しておきながらパソコン起動前にそれを忘却すれば使用不可となるといった愚を犯すおそれもない。勿論、キーボード等の入出力インターフェイスにおけるタイピング情報を記録されてしまうおそれや、目的のサーバーになりすました偽サーバーがWeb画面で入力されたアカウントやパスワードを抽出盗用するといったおそれも全て解消される。

【００３４】さらに上記の効果は、例えばコンピュータの起動から始まって当該コンピュータ内に格納されたアプリケーションプログラムやデータの使用、そして通信回線に接続してインターネットを介した所定サーバーへのアクセス、およびそこでのデータベースアクセスやアプリケーション使用に至るといった、多段階にわたる認証を通じて発揮されるものであり、その使用や管理の簡便性とセキュリティ性の高さは一貫している。

【００３５】つまり、電子デバイスのメモリユニットにそれら各段階において必要となるアカウントやパスワードなどを格納しておけば、各認証段階を正常に完了してはじめて次の段階に進めるよう確実な複数認証が実行される一方、その実行は自動化され使用者に負担となる作業は一切要しないため極めて迅速に処理される。このため、本発明の複数認証方法は、各コンピュータやネットワークに必要とされるセキュリティ性の高低に関わらず様々な状況において適用することができ、その認証対象もコンピュータやサーバーおよびデバイスからアプリケーションプログラムまで実に幅広いものとなるのである。

【００３６】しかして、アカウントやパスワードの管理

が簡便でありながらも高いセキュリティレベルを確実に確保し、サーバー、デバイス、およびアプリケーションプログラムといった多様な認証対象に幅広く適用可能であるＵＳＢインターフェイスを備える電子デバイスを用いた複数認証方法を提供可能となる。

【図面の簡単な説明】

【図１】ＵＳＢキーの外形と使用形態の一例を示す説明図である。

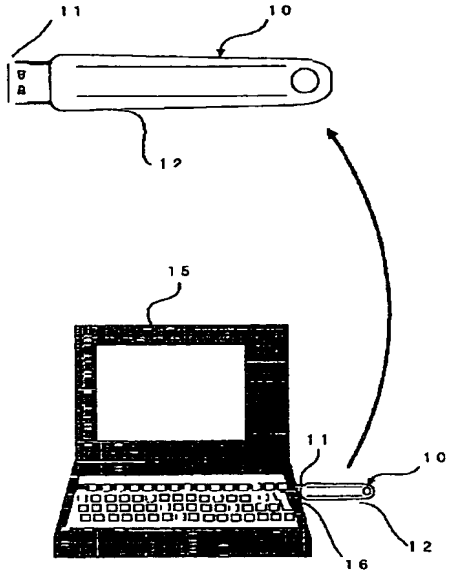
【図２】本発明の複数認証方法を実現するシステム構成例を示す説明図である。

【図３】本発明の複数認証方法の実際手順を示す流れ図である。

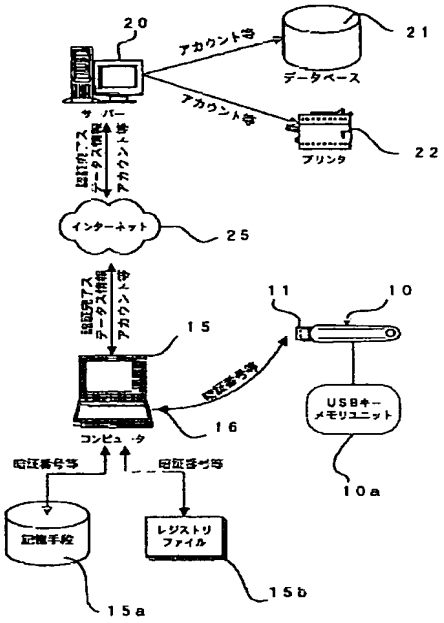
【符号の説明】

１０　電子デバイス（ＵＳＢキー）
１０ａ　メモリユニット
１５　コンピュータ（挿入先コンピュータ）
１５ａ　記憶手段
１５ｂ　レジストリファイル
２０　サーバー
２２　デバイス（プリンタ）

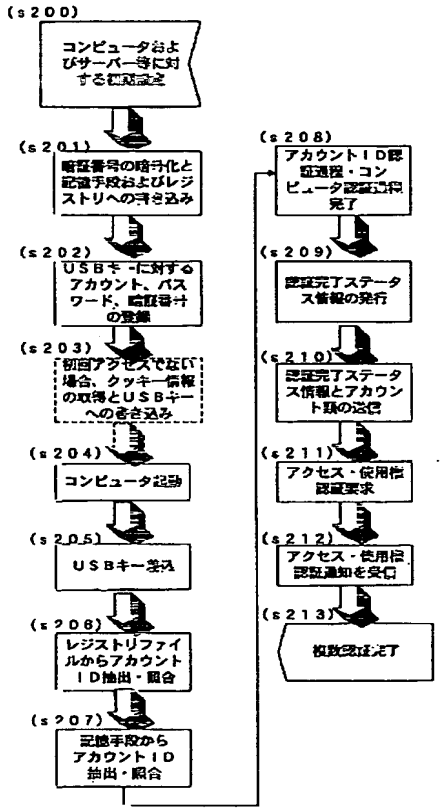
【図１】



【図２】



【図3】


(s200)
コンピュータおよびサーバー等に対する認証設定
(s201)
暗証番号の暗号化と記憶手段およびレジストリへの書き込み
(s202)
USBキーに対するアカウント、パスワード、暗証番号の登録
(s203)
初回アクセスでない場合、クッキー情報の取得とUSBキーへの書き込み
(s204)
コンピュータ起動
(s205)
USBキー差込
(s206)
レジストリファイルからアカウントID抽出・照合
(s207)
記憶手段からアカウントID抽出・照合
(s208)
アカウントID認証過程・コンピュータ認証過程完了
(s209)
認証完了ステータス情報の発行
(s210)
認証完了ステータス情報とアカウント取得の送信
(s211)
アクセス・使用権認証要求
(s212)
アクセス・使用権認証通知を受信
(s213)
複数認証完了